National Institutes of Health (NIH)
E-Authentication Threshold Analysis (ETA)

System Name: ABC System Name (ASN) (Include IC)

National Institutes of Health (NIH)
E-Authentication Threshold Analysis (ETA)

As system documentation is developed for a particular system, an ETA is required to determine if a full E-Authentication Risk Assessment (ERA) is necessary.

The following process guides a System Owner or ISSO through ETA/ERA and documentation, in accordance with OMB M-04-04 and NIST SP 800-63, *Electronic Authentication Guideline*. Each NIH system (including minor children) must have a signed ETA completed and archived in the NIH Security Authorization Tool (NSAT) as part of the SA&A process. If an ERA is required, that document must also be signed and archived in NSAT.

Questions	Yes	No
1. Does the information system require authentication for users to access its data/functionality?	X	
2. Is the system browser based?	X	
3. Is the system external facing? (i.e., is this an information system with users that are connected only to the public Internet?)	X	

Any system that has a "no" response to any one of the three questions does not need an ERA. Only those systems with a "yes" response to all three of the preceding questions need an ERA:

- Requiring authentication
- Being browser based
- Being external facing (with external users that require authentication)

System: ABC System Name (ASN)

Based on the information above, an E-Authentication **is** required. ☒

Based on the information above, an E-Authentication **is not** required. ☐

I agree that the above evaluation is correct.

System Owner Signature	John Doe	Date	8/15/15
System Owner Printed Name	JOHN DOE		
ISSO Signature	John Smith	Date	8/15/15
ISSO Printed Name	JOHN SMITH		
DAA/AO Signature	Sally Smith	Date	8/15/15
DAA/AO Printed Name	SALLY SMITH		

National Institutes of Health (NIH)
E-Authentication Risk Assessment (ERA)

System Name: ABC System Name (ASN) (Include IC)

1. Potential Impact of Authentication Errors:
Indicate the potential impact of the authentication error based on the explanation provided for low, moderate, and high impact below. Please note that a system may have multiple types of transactions (e.g., create, update, delete, read). Therefore, an analysis should be done of the potential impact for each type of transaction.

	Potential Impact Categories for Authentication Errors				
Questions	**Transaction**	**N/A**	**Low**	**Moderate**	**High**
Determine Potential Impact of Authentication Errors					
1. Potential impact of inconvenience, distress, or damage to standing or reputation: **Low:** At worst, limited, short-term inconvenience, distress or embarrassment to any party. **Moderate:** At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party. **High:** Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).	**Create**		X		
	Update		X		
	Delete		X		
	Read		X		
	Highest Impact		X		

2. Potential impact of financial loss: **Low:** At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability. **Moderate:** At worst, a serious unrecoverable financial loss to any party, or a serious agency liability. **High:** Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.	**Create**		X		
	Update		X		
	Delete		X		
	Read		X		
	Highest Impact		X		

National Institutes of Health (NIH)
E-Authentication Risk Assessment (ERA)

System Name: ABC System Name (ASN) (Include IC)

Questions	Potential Impact Categories for Authentication Errors				
	Transaction	N/A	Low	Moderate	High
Determine Potential Impact of Authentication Errors					
3. Potential impact of harm to agency programs or public interests: **Low:** At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests. **Moderate:** At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests. **High:** A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.	**Create**			X	
	Update			X	
	Delete			X	
	Read			X	
	Highest Impact			X	
4. Potential impact of unauthorized release of sensitive information: **Low:** At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS 199. **Moderate:** At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS 199. **High:** A release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS 199.	**Create**			X	
	Update			X	
	Delete			X	
	Read			X	
	Highest Impact			X	
5. Potential impact to personal safety: **Low:** At worst, minor injury not requiring medical treatment. **Moderate:** At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment. **High:** A risk of serious injury or death.	**Create**		X		
	Update		X		
	Delete		X		
	Read		X		
	Highest Impact		X		

National Institutes of Health (NIH)
E-Authentication Risk Assessment (ERA)

System Name: ABC System Name (ASN) (Include IC)

Questions	Potential Impact Categories for Authentication Errors				
	Transaction	N/A	Low	Moderate	High
Determine Potential Impact of Authentication Errors					
6. The potential impact of civil or criminal violations is: **Low:** At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts. **Moderate:** At worst, a risk of civil or criminal violations that may be subject to enforcement efforts. **High:** A risk of civil or criminal violations that are of special importance to enforcement programs.	Create		X		
	Update		X		
	Delete		X		
	Read		X		
	Highest Impact		X		

2. E-Authentication Assurance Level:
Compare the values listed in the "Potential Impact Categories for Authentication Errors" table to the "Maximum Potential Impacts for Each Assurance Level" (below) for each type of transaction.

Maximum Potential Impacts for Each Assurance Level	Assurance Level Impact Profiles			
	1	2	3	4
Determine E-Authentication Assurance Level				
1. Potential impact of inconvenience, distress, or damage to standing or reputation:	Low	Moderate	Moderate	High
2. Potential impact of financial loss	Low	Moderate	Moderate	High
3. Potential impact of harm to agency programs or public interests	N/A	Low	Moderate	High
4. Potential impact of unauthorized release of sensitive information	N/A	Low	Moderate	High
5. Potential impact to personal safety	N/A	N/A	Low	Moderate, High
6. The potential impact of civil or criminal violations is	N/A	Low	Moderate	High

Select the Assurance Level Impact Profile Number (e.g., 1, 2, 3, or 4) for each potential impact that is most closely aligned to the corresponding responses in the "Potential Impact Categories for Authentication Errors" table. In some cases, impact may correspond to multiple assurance levels. For example, a moderate risk of financial loss corresponds to assurance levels 2 and 3. ICs should use the context to determine the appropriate assurance level.

The overall, final assurance level requirement for the information system is the dominant, recurring assurance level for each maximum potential impact.

After the assurance level was determined, follow NIST SP 800-63 to select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance.

National Institutes of Health (NIH)
E-Authentication Risk Assessment (ERA)

System Name: ABC System Name (ASN) (Include IC)

The OVERALL, FINAL ASSURANCE Level is 3

I agree that the above evaluation is correct.

System Owner Signature	John Doe	Date	8/15/15
System Owner Printed Name	JOHN DOE		
ISSO Signature	John Smith	Date	8/15/15
ISSO Printed Name	JOHN SMITH		
DAA/AO Signature	Sally Smith	Date	8/15/15
DAA/AO Printed Name	SALLY SMITH		